UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/938,944	08/24/2001	Trung M. Tran	5181-82200	2680

58467 7590 03/29/2010

MHKKG/Oracle (Sun)
P.O. BOX 398
AUSTIN, TX 78767

EXAMINER	
SHAW, PELING ANDY	
ART UNIT	PAPER NUMBER
2444	

NOTIFICATION DATE	DELIVERY MODE
03/29/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent_docketing@intprop.com
ptomhkkg@gmail.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte TRUNG M. TRAN

Appeal 2009-005937
Application 09/938,944
Technology Center 2400

Decided: March 25, 2010

Before JOHN A. JEFFERY, JOSEPH L. DIXON, and JEAN R. HOMERE, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-25. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellant's invention pertains to controlling data access privileges in a multi-user environment. A directory is populated with entries for each user including various information (e.g., user ID, password, group names, etc.), and an access control list is generated from the directory entries which governs access to particular data sources. *See generally* Abstract; Fig. 6. Claim 1 is illustrative with the key disputed limitation emphasized:

1. A method comprising:

populating a directory with entries for each of a plurality of users of a multi-user computing environment, wherein each entry in the directory comprises a user ID and one or more group names, wherein each of the one or more group names corresponds to a group to which the user ID belongs, and wherein at least one of the entries in the directory comprises a first group name of the one or more group names;

determining a first group access control list for the first group name, wherein the first group access control list comprises the user IDs of users whose entries comprise the first group name, and wherein *the first group access control list is stored outside of the directory*;

for each data source in the multi-user computing environment which permits access by the first group name, granting access to the respective data source to the users in the first group access control list.

The Examiner relies on the following as evidence of unpatentability:

Mangat	US 6,049,799	Apr. 11, 2000
Shandony	US 6,675,261 B2	Jan. 6, 2004

THE REJECTION

The Examiner rejected claims 1-25 under 35 U.S.C. § 103(a) as unpatentable over Shandony and Mangat. Ans. 3-6.[1]

CLAIM GROUPING

Appellant argues the following claim groupings separately: (1) claims 1, 2, 4-11, 13-18, and 20-25, and (2) claims 3, 12, and 19. *See* Br. 5-8. Accordingly, we select claims 1 and 3 as representative of these groups. *See* 37 C.F.R. § 41.37(c)(1)(vii).

CONTENTIONS

Regarding representative claim 1, the Examiner finds that Shandony's "group manager" functionality populates a directory with entries for multiple users having users' IDs and corresponding group names as claimed, but Shandony does not explicitly teach storing a first group access control list outside of this directory. Ans. 4-5.[2] The Examiner, however, cites Mangat as teaching this feature in concluding the claim would have been obvious. Ans. 4, 8, 9.

Appellant argues that neither Mangat nor Shandony stores a group access control list outside the directory as claimed. According to Appellant, any elements in Mangat that could be analogous to an access control list

---

[1] Throughout this opinion, we refer to the Appeal Brief filed January 15, 2008 and the Examiner's Answer mailed March 28, 2008.
[2] *But see* Ans. 8 (noting that while "Shandony does not *seem* to show explicitly" storing the group access control list outside of the directory, Shandony's separate user and group manager functions "*may*" nonetheless teach the limitation) (emphases added).

(i.e., group object, membership list, association lists, and access rights) are stored within the directory services server, and therefore Mangat allegedly teaches away from the claimed invention. Br. 6.

Appellant adds that Shandony likewise fails to store a group access control list outside the recited directory. *Id.* Although Appellant acknowledges that Shandony's group manager permits modifying group access privileges, it is associated with an identity server that merely provides a user interface for data stored in the directory server. *Id.*

Regarding representative claim 3, Appellant argues that Shandony does not teach or suggest granting access to the data source to one or more users whose directory entries comprise a first hostname, and who are seeking access from the host having the first hostname. Br. 7-8.

The issues before us, then, are as follows:

ISSUES

1. Under § 103, has the Examiner erred by finding that Shandony and Mangat collectively would have taught or suggested:

(a) storing a first group access control list outside of the directory containing users' IDs and corresponding group names as recited in claim 1?

(b) granting access to the data source to one or more users (1) whose directory entries comprise a first hostname, and (2) who are seeking access from the host having the first hostname as recited in claim 3?

2. Is the Examiner's reason to combine the teachings of these references supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

FINDINGS OF FACT (FF)

1. Shandony discloses a system that provides identity and access management services for a network via (1) an "Identity System" that manages identity profiles, and (2) an "Access System" that provides security for resources across web servers. Shandony, col. 5, ll. 23-30; Fig. 1.

2. The Access System includes Access Server 34, Web Gate 28, and Directory Server 36. Access Server 34 not only provides authentication, authorization, and auditing services, but also identity profiles that are used across multiple domains and Web Servers from a single web-based authentication (sign-on). Shandony, col. 6, ll. 52-57; Fig. 1.

3. The Identity System includes Web Pass 38, Identity Server 40, and Directory Server 36. Identity Server 40 manages identity profiles for: (1) individual users via "User Manager" 42; (2) groups via "Group Manager" 44; and (3) organizations via "Organization Manager" 46. Shandony, col. 6, l. 64 – col. 7, l. 11; Fig. 1.

4. User Manager 42 handles the functions related to user identities and access privileges, including creating and deleting user identity profiles, modifying user identity profile data, determining access privileges, etc. Shandony, col. 7, ll. 20-25; Fig. 1.

5. Group Manager 44 allows entities to create, delete, and manage groups of users who need identical access privileges to resources. To this end, the Group Manager allows adding and deleting users from established groups. Shandony, col. 7, l. 64 – col. 8, l. 11; Fig. 1.

6. An "identity profile" is a set of information associated with a particular entity (e.g., user, group, organization, etc.). The data elements of identity profiles are "attributes," and may include a name, value, and access criteria. Shandony, col. 6, l. 66 – col. 7, l. 4.

7. Examples of attributes stored in a user identity profile include the user's name, telephone number, identification of work facility, organization that the user works for, department number, department URL, etc. Shandony, col. 13, ll. 54-64.

8. Examples of attributes stored in a group identity profile include the owner, name, description, "static members,"[3] "dynamic member" rule, subscription policies, etc. Shandony, col. 13, ll. 64-67.

9. Shandony's Figure 5 shows an exemplary hierarchical directory tree that can be stored on Directory Server 36. Each node on the tree is an entry in the directory structure that includes an identity profile. The entity can be a user, group, or organization. Shandony, col. 14, ll. 4-50; Fig. 5.

10. Shandony's Figure 12 shows how identity profiles are accessed. Upon receiving a request from a user's browser, the appropriate manager (i.e., the User Manager 42, Group Manager 44, or Organization Manager 46) accesses (1) a "target profile" (i.e., the identity profile sought to be viewed), and (2) a "source profile" (i.e., the requesting user's identity profile) on directory server 36. The appropriate manager then determines access rights

[3] A "static member" is explicitly identified as a member, unlike a "dynamic member" that is indirectly identified by a rule or other means. Shandony, col. 36, ll. 59-61.

for the target profile's attributes and, based on this determination, passes appropriate results to the user's browser. Shandony, col. 18, l. 49 – col. 19, l. 1; Fig. 12.

11. Mangat's system manages links between documents and other data structures (e.g., applications), and includes a user (client) station 56 connected to (1) file server 58, and (2) directory services server 60, respectively, via network 30. Mangat, Abstract; col. 5, ll. 1-15; col. 5, l. 57 – col. 6, l. 22; Figs. 1-2.

12. The directory services server 60 includes a "user object" 128 that may include (1) certain attributes related to users' rights 134 to access documents 144 on file server 58, and (2) an "association list" 136 that may include identifying information related to associated documents 144. Mangat, col. 12, ll. 34-43; col. 15, ll. 10-43; Figs. 2, 4.

13. The directory services server 60 also includes a "group object" 120 that identifies members of a group and has associated rights 116 and a membership list 124. The group object also includes an access control list 202 that may identify objects 113 having access to the group object's association list 200 or the group object. Mangat, col. 12, ll. 25-33; col. 16, ll. 13-40; Figs. 2, 5.

14. Shandony's Figure 69 details the access server's determining whether a resource URL matches a specific policy URL. In this determination, Web Gate 28 sends the access server data associated with an HTTP POST request (e.g., via an online form containing POST data), and

assesses whether there is a match between the received POST data and the POST data required by the policy. Shandony, col. 5, ll. 7-8; col. 71, l. 48 – col. 72, l. 4; Fig. 69.

15. An internet domain can reside on a single Web Server or be distributed across multiple Web Servers. Shandony's Access System therefore allows a user to satisfy the authentication requirements of plural domains and/or Web Servers by performing a single authentication. Shandony, col. 72, ll. 5-12.

PRINCIPLES OF LAW

To be patentable under § 103, an improvement must be more than the predictable use of prior art elements according to their established functions. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). Moreover, if a technique has been used to improve one device, and an ordinarily skilled artisan would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. *Id.*

ANALYSIS

Claims 1, 2, 4-11, 13-18, and 20-25

We find no error in the Examiner's conclusion that Shandony and Mangat collectively would have taught or suggested storing a first group access control list outside of the directory containing users' IDs and corresponding group names as recited in claim 1.

We note at the outset that the Examiner seemingly takes alternative positions regarding whether Shandony alone teaches this disputed feature. *Compare* Ans. 4-5 (noting that Shandony does not explicitly teach storing a first group access control list outside of the recited directory) *with* Ans. 8 (noting that Shandony's separate user and group managers "may" teach this feature).

Despite this inconsistency, we nonetheless agree with the Examiner that Shandony and Mangat collectively would have taught or suggested the disputed limitation, particularly in view of the scope and breadth of claim 1. All claim 1 requires in this regard is storing the first group access control list "*outside*" of the directory. Nothing in this language requires storing the list in separate servers or storage devices. Rather, the limitation is fully met so long as the access control list is stored "outside" of the directory (e.g., stored separately from the directory). Notably, nothing in the claim precludes this separate storage as residing on the same storage device (e.g., different files on a server, etc.).

Turning to Shandony, User Manager 42 and Group Manager 44 both (1) are located in Identity Server 40, and (2) access respective identity profiles that are stored on directory server 36. FF 3 and 10. And these identity profiles (whose functionality is managed by User Manager and Group Manager) include various attributes pertaining to users and associated groups, as well as access criteria. *See* FF 4-9.

Even assuming, without deciding, that these identity profiles and associated access control information are stored exclusively in Shandony's directory server (and therefore distinct from the user and group management functions in the identity server) (*see* FF 3 and 10), nothing in the claim

precludes this storage. That is, even assuming that the group profile information ("directory") and corresponding access control information for particular users within that group resided solely in the directory server, Shandony at least would have suggested that these items of information would be stored separately on that server. *See* FF 3-8 and 10. In any event, Appellant has not shown that storing these respective items on different servers (e.g., the directory server and identity server) would have been an unpredictable variation beyond the level of ordinarily skilled artisans. *See KSR*, 550 U.S. at 417.

Although Mangat is merely cumulative to Shandony in this regard, we nevertheless find no error in the Examiner's reliance on Mangat. Here again, nothing in claim 1 precludes Mangat's separately storing a "user object" and "group object" and their respective access rights and associated lists on the same server (i.e., the directory services server 60). *See* FF 11-13. Appellant's arguments in this regard (Br. 6) are simply not commensurate with the scope of the claim. That Mangat explicitly states that this group object includes a distinct *access control list* 202 (FF 13) only bolsters our conclusion that Mangat at least would have suggested storing this list outside of the directory as claimed.

Based on these teachings, we find the Examiner's reason to combine the teachings of Mangat with Shandony supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion.

We are therefore not persuaded that the Examiner erred in rejecting representative claim 1, and claims 2, 4-11, 13-18, and 20-25 which fall with claim 1.

Claims 3, 12, and 19

We will also sustain the Examiner's rejection of representative claim 3 which calls for, in pertinent part, granting access to the data source to one or more users (1) whose directory entries comprise a first hostname, and (2) who are seeking access from the host having the first hostname.

We find no error in the Examiner's reliance (Ans. 9) on Shandony's authentication system which examines submitted "POST" data (e.g., via an online form containing POST data). FF 14. The access server uses this POST data to determine whether a resource URL matches a specific policy URL, namely by assessing whether there is a match between the received POST data and the POST data required by the policy. *Id.*

Since (1) a URL may include a hostname as Appellant admits (Br. 8), and (2) POST data is used to determine a requisite match between URL information as noted above (*id.*), we see no reason why this submitted POST data could not include the name of the host from which the user seeks access to that resource in this determination. Including this hostname information in directory entries would have been well within the level of ordinarily skilled artisans, particularly since Shandony's identity profiles can contain a wide variety of information pertaining to users, including URL information. *See* FF 7-8.

We are therefore not persuaded that the Examiner erred in rejecting representative claim 3, and claims 12 and 19 which fall with claim 3.

CONCLUSION

The Examiner did not err in rejecting claims 1-25 under § 103.

ORDER

The Examiner's decision rejecting claims 1-25 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

MHKKG/Oracle (Sun)
P.O. BOX 398
AUSTIN, TX 78767